

# I.T. Security

## Is your I.T. Security keeping you up at night?

The important and commercially sensitive information kept on computers just keeps growing and employee identity theft is now at epidemic proportions. Organised crime is becoming more and more sophisticated, so security often falls behind.

This can leave companies open to blackmail from hackers or internet pirates using botnets, a network of computers programmed to work in concert to overload a target computer's capability. There is also the threat from revenge by ex-employees – this may come via IT based viral attack, or people walking off with laptops containing sensitive information.

### Think security

Do your employees leave their computers on at night or leave their password on a Post-It note stuck to their computers?

Security vulnerabilities from outsourced operations can also be a risk – especially if these are based abroad. That's why businesses must not just insist on high levels of security from business partners, but check and monitor these regularly as well.

Linked systems also cause problems as one lax area of security threatens all those in the chain; wireless access is also a major risk.

### So what can you do?

One decision that can help you establish an adequate security level is to work to a standard such as BS7799.

This involves the following steps:

1 Security policy: Sets out the high level principles a business has for protecting data – creating a document used to educate employees.

2 Organisation security: Deals with the nuts and bolts of how information security management is organised.

3 Asset classification and control: Ensures information and information-processing equipment are managed and accounted for as valuable assets.

4 Personnel security: Covers any personnel issues such as training responsibilities, vetting procedures and how staff should respond to security issues.

5 Physical and environmental security: Looks at physical aspects of security including protection of equipment and information from physical harm.

6 Access control: Control of access to information and systems on the basis of business and security needs.

7 Communications and operations management: Examines correct management and secure operation of information processing facilities during day-to-day activities.

8 System development and maintenance: To ensure security and the maintenance of information integrity.

9 Business continuity management: Ensures the maintenance of essential business activities during adverse conditions. From major disasters to minor local issues.

10 Compliance: Concerns business compliance with relative national and international Law, professional standards and any processes mandated by the information security management system.

The BS7799 Standard is a good supplement to guard against computer crime but is no substitute for adequate insurance.



## Need to know more?

For more information contact Colin Bailey or Andrew Milverton on 0118 940 6175 at Cassey Miller James.

Details of our offices and telephone numbers can be found on our website at [www.cmj.co.uk](http://www.cmj.co.uk)

Any views or opinions expressed in this briefing are for guidance only and are not intended as a substitute for appropriate professional advice.

We have taken all reasonable steps to ensure that the information contained herein is accurate at the time of writing but it should not be regarded as a complete or authoritative statement of law. Cassey Miller James Ltd is authorised and regulated by the Financial Services Authority.